Superseded by FIPS 65

NBSIR 77-1228

Automatic Data Processing Risk Assessment

Susan K. Reed

Systems Architecture Section
Systems and Software Division
Institute for Computer Sciences & Technology
National Bureau of Standards
Washington, D. C. 20234

March 1977

Interim

U. S. DEPARTMENT OF COMMERCE
NATIONAL BUREAU OF STANDARDS

NBSIR 77-1228

AUTOMATIC DATA PROCESSING RISK ASSESSMENT

Susan K. Reed

Systems Architecture Section
Systems and Software Division
Institute for Computer Sciences & Technology
National Bureau of Standards
Washington, D. C. 20234

March 1977

Interim

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, *Secretary*

Dr. Betsy Ancker-Johnson, *Assistant Secretary for Science and Technology*

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Acting Director*

TABLE OF CONTENTS

PREFACE

The method described here is based in part on the work of several members of Federal Information Processing Standards Task Group 15, Computer Systems Security. The National Bureau of Standards is grateful to Robert H. Courtney, Jr., of the IBM Corporation for his kind permission to adapt his work to the needs of the Federal Government and for his continuing assistance. Also from Task Group 15, the work of T. Q. Stevenson of the Department of Agriculture and Ralph E. Gooch of the Bureau of the Census to design an entire risk analysis process which requires a minimal resource investment is greatly appreciated. This document draws upon some of this material and their jointly developed example for illustrative purposes is a component of this presentation. The list of application system vulnerabilities was formulated by Dr. Theodore A. Linden and Dr. Stuart W. Katzke of the National Bureau of Standards.

This publication has been prepared for use by Federal agencies in response to an expressed need. It is an interim document. The author particularly desires to know of difficulties, questions or successes in its use which could lead to a revision. Further refinement and expansion of this document are planned, based on experience.

Address:	Room A-265, Technology Building National Bureau of Standards Washington, D.C. 20234
Phone:	(301) 921-3861

AUTOMATIC DATA PROCESSING RISK ANALYSIS

Susan K. Reed

This document presents a technique for conducting a risk analysis of an ADP facility and related assets. Risk analysis produces annual loss expectancy values based on costs and potential losses estimated by a management-appointed team from within the organization using and maintaining the ADP facility. The annual loss expectancy values are fundamental to the cost-effective selection of safeguards for the security of the facility. For the purpose of clarity, the ADP facility of a hypothetical Federal agency is used for an example. The characteristics and attributes which must be known in order to perform a risk analysis are described and the process of analyzing some of the assets is demonstrated, showing how the problem of risk analysis can be reduced to manageable proportions.

Key Words: ADP availability; annual loss expectancy; application system vulnerability; computer security; data confidentiality; data integrity; data security; physical security; procedural security; risk analysis; risk assessment; systems security

1. INTRODUCTION

Hand in hand with the increase in awareness of the need for computer security has come the need for a method of quantifying the impact of various adverse situations on the functioning of organizations supported by automatic data processing. Risk analysis involves consideration of missions and tasks in the light of physical environment, personnel, equipment, content of files and performance capability. There are any number of techniques for performing such analyses but always to be considered vis-a-vis each other are the two key elements:

1. The damage which can result from an event of an unfavorable nature.

2. The likelihood of such an event occurring.

A risk analysis provides management with information on which to base decisions, e.g., whether it is best to prevent the occurrence of a situation, to contain the effect it may have, or simply to recognize that an adverse potential exists. Because a risk analysis is the basis for such decisions, its findings of loss or damage must be presented in a quantitative, comparable fashion.

The goal of a risk analysis is to strike an economic balance between the impact of risks and the cost of protective measures. It serves to point out the risks which exist but not to develop the protective measures required. First of all an analysis shows the current security posture in an organization, then it points out where greater (or less) security is needed, and, finally, it assembles some of the facts needed for the selection of adequate, yet cost effective, safeguards. A secondary benefit of a risk analysis is the increased security awareness which will be apparent to all organizational levels from management through operations.

Risk analysis is not a task to be accomplished once for all time. It must be performed periodically in order to stay abreast of changes in mission, facilities and equipment. And since security measures designed at the inception of a system have generally proved to be more effective than those superimposed later, risk analysis should have a place in the design phase of every system.

The major resource required for a risk analysis is manpower. For this reason the first analysis will be the most expensive, as subsequent ones can be based in part on previous work and the time required will decrease to some extent as experience is gained.

The time allowed to accomplish the risk analysis should be compatible with its objectives. Large facilities with complex, multi-shift operations and many files of data will require more time to complete than the single shift, limited production locations. If meaningful results are expected, management must be willing to commit the resources necessary for accomplishing this undertaking.

2. THE ROLE OF MANAGEMENT IN RISK ANALYSIS

2.1 Management

The eventual success of a risk analysis will be strongly contingent on the role top management takes in the project. Necessary will be:

1. Management <u>support</u> of the project expressed to all levels of the organization

2. Management delineation of the purpose and scope of risk analysis

3. Management selection of qualified team and formal delegation of authority

4. Management review of team's findings

Personnel who are not directly involved in the analysis process must be prepared to provide information and assistance to those who are conducting the analysis and, in addition, to abide by any procedures and limitations of activity which may ensue. Management should leave no doubt that it intends to rely on the final product and base its security decisions on the findings of the risk analysis team. The scope of the project should be defined to encompass ADP users (this will probably include all departments and any users outside the organization) as well as the actual ADP facility, equipment and personnel.

2.2 Risk Analysis Team

The selection of the individuals who will comprise the risk analysis team is critical to the outcome of the project. It is important to obtain representation from the components responsible for the following:

ADP operations management
System programming (if separate from ADP operations)
Internal auditing
Physical security
Data under consideration
Programming support of the data under consideration.

These entities should be represented on the team by senior people, well-informed of their own component's mission and its relationship to the overall organizational mission. The task team leader should be equally knowledgable and should come from one of the first three above listed components, but should not be that component's representative. In other words, the team leader should not wear two hats--one as leader and one as a representative.

The team leader and the members should be designated in writing and their duties, responsibilities and any accompanying authority should be outlined. It should also be understood that the job cannot be done adequately if alternates are assigned.

2.3 Allocation of Time

Risk analysis is a time-consuming process, and one which cannot be hastened. Experience helps considerably; having all the necessary information readily available is also a help, as is the use of well-designed forms. At best, the consideration of each data set or file

in the light of the hazards which beset a system is a tedious business, but one which should only be delegated to subordinates with great deliberation because of the level of knowledge and experience required in the decision process. It can be a very enlightening task however.

In industry it has been estimated that 2000 data files a month is about the limit which can be considered even under optimum conditions. An organization's first risk analysis will probably not be conducted under optimum conditions.

Assignment to the team will create hardship on organization components, which will be forced to do without the services of useful, motivated personnel, as well as on the team members, who will feel constrained to rush through the risk analysis in order to hurry back to their normally-assigned duties. An agreement that the team will meet only half of each day would alleviate much of these burdens.

2.4 Management Review

Top management should review the findings of the risk analysis team before a protection plan is formulated.

3. PRELIMINARY EXAMINATION

In order to have a firm basis for conducting the risk analysis, it is wise to initiate the project with a look at the facility's existing security. This examination should aim at identification and review of existing protective measures rather than evaluation of their adequacy, since a true evaluation can only be based on the consideration of the impact of threats vis-a-vis the probability of their occurrence. Such a survey will, however, give management an overview of the current security posture. It may also point to the need for temporarily implementing certain elementary safeguards until a complete security plan based on the risk analysis can be conceived and implemented.

Following the plan outlined in the Guide to Computer Security Inspection and Evaluation [6] will provide Management with a review of all the features and measures in effect which could contribute to facility or data security even though their original purpose may not have been protective, e.g., storage media usage logs, control of printout distribution, data entry quality controls. (It will, in fact, be seen that most good management practices promote security.)

An additional product of the preliminary examination should be a list of the replacement costs, or best estimates thereof, of tangible assets, i.e., the computer(s) and all related equipment, data, buildings, etc. In addition to the normal considerations for life safety, it should

be remembered that people are an asset which cannot easily be replaced because of the training and experience they bring to their jobs.

4. RISK ANALYSIS

4.1 Elements

The essential elements of a risk analysis are an assessment of the damage which can be caused by an unfavorable event and an estimate of how often such an event may happen in a specified period of time. The product of these two will be a statement of expected damage per unit of time.

4.2 Tools

Necessary to performing a risk analysis are a quantitative means of expressing potential impact and a logical means of expressing estimated frequency of occurrence which will admit dealing comparably with both very low and very high frequency events.

4.2.1 Expression of Impact

To date, no better common denominator has been found for stating the impact of an adverse circumstance--whether the damage is actual or abstract, the victim a person, a piece of equipment or a function--than monetary value. While there will be those who feel that equating financial impact with human suffering and misfortune is a callous exercise in quantification, it is nevertheless the recompense accepted in civilized societies, used even by the courts to redress physical and mental anguish.

4.2.2 Expression of Frequency

Because budgets, along with most financial matters, are organized on an annual basis, a year is obviously the most suitable time period to specify in expressing expected frequency of occurrence of threats. There are, however, some threats which actually occur only once in a number of years and others which happen regularly many times a day. It is not easy to say that something happens every 1/73 year instead of five times a day, nor is it easy to work with such fractions. For this reason the transmutation of a thousand days to three years, etc. (as shown in figure 1) has been evolved. It will avoid the use of unwieldy fractions, yet maintain the flexibility to work with high probability events in days and low probability events in years.

4.2.3 Additional Aids

In a risk analysis, it is neither necessary nor desirable to make precise statements of impact and probability. The time needed for the analysis will be considerably reduced, and its usefulness will not be decreased, if both impact and frequency statements are given in factors of 10. In other words, there will be no significant difference in the overall evaluation of threats whether the damage from a certain event is estimated at $120,000 or $165,000 nor whether its anticipated frequency is twelve or fifteen times a year. If at the time of selecting safeguards it becomes important to refine specific items, that can be done, but during the analysis phase gross statements are all that are required. In order to assist the team in taking advantage of this relaxation of preciseness, the conversion tables in figure 1 have been prepared. Their use will simplify the team's work and thus decrease the time they must spend on it.

If the cost impact of the event is

$10, let i = 1
$100, let i = 2
$1,000, let i = 3
$10,000, let i = 4
$100,000, let i = 5
$1,000,000, let i = 6
$10,000,000, let i = 7
$100,000,000, let i = 8

If the estimated frequency of occurrrence is

Once in 300 years, let f = 1
Once in 30 years, let f = 2
Once in 3 years, let f = 3
Once in 100 days, let f = 4
Once in 10 days, let f = 5
1 per day, let f = 6
10 times per day, let f = 7
100 times per day, let f = 8

Figure 1. Selection of Values

Annual loss expectancy (ALE) is the product of impact and frequency. When using the values of f and i derived from the conversion tables, the value of ALE may be approximated by the formula:

$$ALE = \frac{10^{(f+i-3)}}{3}$$

No weighting factors have been introduced into the formula; the change is only for the purpose of accommodating the converted values.

An even faster way to determine ALE is to use the matrix shown in figure 2.

Values of f

Values of i	1	2	3	4	5	6	7	8
1					$300	$ 3K	$ 30K	$300K
2				$300	3K	30K	300K	3M
3			$300	3K	30K	300K	3M	30M
4		$300	3K	30K	300K	3M	30M	300M
5	$300	3K	30K	300K	3M	30M	300M	
6	3K	30K	300K	3M	30M	300M		
7	30K	300K	3M	30M	300M			

Values of ALE

Figure 2. Determination of Annual Loss Expectancy (ALE)

4.3 Technique

It would be difficult to list all the undesirable events which could have a deleterious effect on data processing. Nevertheless, a thorough understanding of these vulnerabilities is required on the part of those conducting the risk analysis. A partial list of such vulnerabilities is presented in Appendix A. The risk analysis team can use this list to assure that they maintain a balanced view of the various vulnerabilities. If the composition of the risk analysis team is an appropriate one, the members will be able to think of specific instances where these vulnerabilities apply to their agency's system. Furthermore, some member of the team should be able to think of additional vulnerabilities in each of the categories covered in the Appendix.

SYSTEM/APPLICATION	DATA INTEGRITY		DATA CONFIDENTIALITY	PROCESSING AVAILABILITY			COMMENTS
Data Files	Modification	Destruction		* 2 hrs	* 24 hrs	* 72 hrs	
	(i) (ALE) (f)	(i) (ALE) (f)	(i) (ALE) (f)	(1) (ALE) (f)	(i) (ALE) (f)	(i) (ALE) (f)	

*The delay times in these columns must be established by each organization for itself in accordance with its mission. The figures shown above are for example only.

To prevent the risk analysis from bogging down in the detail of a formal vulnerability study, the risk analysis should focus on the potential results of these undesirable events, i.e., on the harm which they could cause. With this approach, the task will assume feasible proportions.

The kinds of harm which can befall automatic data processing facilities are easily categorized:

1. Those which cause loss of data integrity
2. Those which cause loss of data confidentiality
3. Those which cause loss or delay in automatic data processing availability

The key terms are defined as follows:

DATA INTEGRITY - The state that exists when computerized data is the same as that in the source documents or has been correctly computed from source data and the data has not been exposed to accidental or malicious alteration or destruction. Incomplete data, fictitious changes or additions to the data, and erroneous source data are also considered violations of data integrity.

DATA CONFIDENTIALITY - The status of data that is held in confidence and is protected from unauthorized disclosure. Misuse of data by those authorized to use it for limited purposes is also considered a violation of data confidentiality.

ADP AVAILABILITY - The assurance that required ADP services will be available within an acceptable period of time even under adverse circumstances.

All of the organization's data files, aggregated by system or major application area with which used, should be listed down the left side of a worksheet like the one shown in figure 3 (enlarged to provide more working space). If a file is used with more than one system, it should be listed under each, as it may be vulnerable to different hazards under different systems. Such multiple listings should be noted in the Comments column.

By considering the exercise given each file by the application, it should be possible to identify the states in the processing where circumstances--including natural hazards--can occur which would affect the security or availability of the file and to assign reasonable estimated frequencies to such events. The converted values of i and f should be filled in at each intersection, as should the value of ALE, otherwise it will be impossible to reconstruct the basis for a particular ALE, if that becomes necessary. Where more than one circumstance can affect the

data integrity, data confidentiality or processing availability, the i and f values for each should be noted separately; this will be an aid in deciding on security measures. Use the Comments column to note the steps or functions in a system where problems can occur. When considering data confidentiality, the task can be simplified by first identifying the files which are known to contain no personal, proprietary or other information of a nature which would make disclosure a problem.

In considering data integrity, the further division into modification and destruction is necessary because the impact and frequency will not always be the same.

The time periods in the Processing Availability column are mission dependent and will have to be determined by each individual organization. They will be important in the selection of back-up facilities and should be subject to particular review by top management.

4.4 Advice, Common Sense and Helpful Hints

The comments in this section are based on experience (mostly in the private sector). They are included in the hope that they will place some of the difficulties attendant on a risk analysis in the proper perspective and give the team confidence in its own collective judgment.

4.1.1 Human Frailty. The team will come upon doubts as they weigh the part personal integrity plays in the security of a system. While every Federal employee who works in an ADP environment should have a clearance appropriate to the content or purpose of the pertinent systems, there is no way of knowing at any time what stresses are operating on an individual--what pressures he has at home, what jealousies exist in the work situation, what financial burdens he is under. For these reasons, it is usually best to eliminate individual personal integrity from consideration in a risk analysis. The right time for considering personal integrity is during the development of the security plan, when such measures as pre-employment investigation, appropriate clearances, rotation of duties, acting in concert, etc. can be discussed.

There are several other well documented facts in the same vein:

- The vast majority of white collar crime is committed by employees defrauding their own employers
- In general, employees who defraud their employers do so using resources to which they have access in the course of their jobs
- The best deterrent to white collar crime has proved to be curtailment of incentive, i.e., limiting the profit potential of dishonest activity to the minimum

consistent with the assigned task. If employees can expect no more than minimal gain from unscrupulous acts, they will be less likely to attempt them. The second best deterrent is the fear of getting caught. If employees know there is adequate surveillance of activity they will be less apt to place themselves in jeopardy.

4.4.2 Physical Security and Inability to Process. Another difficulty the team could encounter would be the confusion caused in treating fires, floods and other natural disasters solely as physical security problems, thus falling into the trap of trying to solve them with physical security measures alone. While the initial impact of natural disasters is usually physical destruction, there can be other less immediately obvious effects on processing capability, such as loss of utilities and damage to data storage media. There can also be loss of services without any damage to a facility.

The loss of the physical facility and the loss of processing availability should be treated independently of each other, since neither is tantamount to the other. The loss of the physical facility need not mean total loss of processing availability if the functions which are truly critical to the agency mission are supported by a prearranged, alternate facility. It would probably not be possible to find a processing facility capable of assuming an agency's entire ADP workload but, working under special interagency, mutually beneficial agreements, the 10% to 15% of the workload which is vital can be performed elsewhere. Plans for such contingencies should cover the availability at the alternate facility of everything necessary to processing including forms, programs, communications, data, personnel, etc.

The total inability to process data can be caused by other circumstances than physical destruction. For instance, hardware malfunctions can hold up all processing for several days; accidental erasure of critical programs or data can delay an urgent task for many hours; a fire in another part of a building can deprive the ADP center of all utilities; water logging of preprinted output forms can halt output until the forms can be replaced, possibly a matter of weeks. Water damage can result not only from overflowing rivers, but also from leaking pipes, bursting pipes or fire quenching activity nearby.

4.4.3 Estimating Frequency of Occurrence. At first the team may feel that estimating frequency of events for which there is no history of occurrence is imponderable. Common sense, however, can rescue them from their dilemma.

For example, consider a payment system which processes many different options. There may be good automated controls over the number of checks, the amounts of the checks, and the sums of the amounts of the checks; however, several hundred people may know that it is relatively easy to change a recipient's address without risk that it will be detected. In such a situation, one of them may divert checks to an address where they can be picked up and cashed by someone other than the intended recipient. Such a situation should yield an estimated frequency much higher than once in 30 years and probably much lower than once every 10 days, leaving the choice between once every three years or once every hundred days. Selecting the most appropriate figure depends on several factors, including the general atmosphere in which the system functions. If the number of people who know of the exposure is one or two hundred, the former is the most likely figure. If the number of people who know is nearer a thousand, or if the employee dishonesty is accepted by management so long as it stays within established bounds, then the higher estimated frequency would be correct. This selection must be left to the risk analysis team.

Understanding the interaction of the factors which impact frequency estimation is one of the reasons for selecting the team members as suggested in Chapter 2. These factors, which are hardly ever discrete and unrelated, include:

- Access. Is access to processing local or remote? Can an intruder gain access to processing, to data, to software, to equipment, to storage media, to supplies, to documentation, to output, to trash? Can an employee do the same? Accidentally? Maliciously? etc.

- Natural Disasters. What kinds of natural disasters might reasonably be expected to occur? To what extent will the facility be affected? Processing? Data? Supplies? Loss of utilities? etc.

- Environmental Hazards. What special hazards are nearby? Explosives, flammable products? Unused or unguarded buildings? What can be the aftermath of fire? Water damage? Loss of utilities? Exposure of data? Loss of processing capability? Promimity of fire department? etc.

- Facility Housing. Is ADP facility in separate building? Who administers it? Who protects it? What construction is it? What protective devices are installed? How close is it to heating equipment? Cooking equipment? Other fire hazards? What kind of ceiling? What kind of flooring? etc.

- <u>Personnel and Work Environment</u>. What is relationship between personnel and management? Loyal? Suspicious? What are aggrevations of employees? Satisfactions? How well do supervisors know personnel? What is management attitude toward employee dishonesty? Condone, within bounds? Are lines of communication open between individual employees and supervisors? Employees and senior management? etc.

- <u>Value</u>. How much can an intruder gain by penetrating the system? Disclosing data? Disrupting operations? How much can an employee gain? How much can a subject be hurt by unauthorized disclosure of data? How much can the organization be hurt? How much by incorrect data? etc.

5. AN EXAMPLE

The hypothetical government agency described here has been developed to show some of the facets which must be considered in a risk analysis. The applications discussed here are not intended to represent the agency's entire ADP operation. In reality, they would probably comprise only a very small part.

5.1 General Environment

5.1.1 Central Computer Facility

- The central ADP facility is housed in a separate 3-story wing of the agency's headquarters which is located in central Kansas.

- The equipment consists of a large scale processor with 3 CPUs, 32 tape drives, 10 billion characters of disk storage, 3 front end communications processors capable of handling 175 terminals (125 are presently in the system), a COM unit and a library of 50,000 reels of tape.

- Guards check all personnel into and out of the computer area. Badges are required. Areas not monitored by guards are controlled by an electronic card system. Procedures are in effect covering lost, forgotten, stolen and damaged badges and card passes and the issuance of badges to visitors.

- There is a supervised fire detection/suppression system consisting of products-of-combustion detectors and a dry-pipe sprinkler system. Hand extinguishers are located throughout the facility, the type determined by the equipment or supplies in their vicinity. Continuing emergency team training is required of all computer operations personnel. The training includes actual use of the various extinguishers. Fire safety orientation is given to all employees when first hired and annually thereafter. Areas of the building adjacent to the computer facility do not have fire detection devices. These areas are under the control of operating units other than data processing.

- There is no emergency power or uninterruptable power supply backup. In the last seven years the facility has experienced machine failure due to power outages resulting from thunder storms, fire at the utility substation and breaks in the main power feeder caused by a construction project. In recent months (especially summer) local brownouts have caused the failure of certain electronic equipment. These brownouts occur about every three weeks.

- The air conditioning unit is five years old and has suffered three breakdowns: one 2 years after installation, one 18 months later, and a third after another year. Two 100-ton cooling towers are located on the roof of the wing in which the ADP facility is located.

- Plastic covers are supplied for all hardware in the facility. The flooring is raised 24 inches and there are automatic pumps in case of water entry. The tape library is well protected from water damage.

- Emergency power-down switches are provided for all computer and air conditioning systems.

- Management is aware that, annually, about 400 tape and/or disk files are misplaced or destroyed by incorrect handling or overwriting because of improper labeling.

- Employee morale is notably high. The agency has established good personnel policies and the procedures for dealing with employee complaints work fairly and to everyone's satisfaction. All ADP personnel are aware of management's continuing interest in maintaining and enforcing security procedures at both central and remote facilities.

- The operating system must be restarted several times a week. Sometimes the problem can be traced to a hardware failure, but usually it is not resolved. Systems programmers maintain the system with little direct supervision. There is no formal review before changes are installed. The operators have learned how to keep the system running efficiently, but some of the evening and night supervisors have little understanding of what the operators do.

5.1.2 Terminals

- The remote job entry terminals are all located in GSA leased spaces, one at each field office. They are locked when unattended; however, they are used be several branches of the agency for a number of systems. Magnetic tapes are secured in locked cabinets located in terminal rooms. Data tapes are retained for one month only. Source documents on microfilm are stored in secure areas other than in the terminal room. Communication lines are not protected.

5.1.3 Back Up Facilities

- No plans have been made for emergency backup of automatic data processing.

5.2 Specific Systems

5.2.1 Application-100. This application supports a mission stemming from an Executive Order requiring a report to be produced and published on the third Thursday of each month. It has been automated for ten years. A master file containing the most recent report must be updated monthly with new data transmitted from 30 field offices to the central facility. When the new data are merged, a new report is produced and distributed through controlled official channels.

The following set of circumstances is assumed for this application:

- The data are necessary to the Federal community. Their output can have an economic impact on the private sector if released early.

- At the field offices the source documents are microfilmed after data have been translated into machine readable format (magnetic tape). Seven of the offices have their own microfilming equipment; twenty-three have it done on contract.

- Data are transmitted by private leased lines to central facility for processing. Transmission is accomplished during third shift operation (0001 to 0800) Tuesday.

- If communications network is down, data tapes are flown to the central facility. Communications failure occurs an average of three times a year.

- Only ADP personnel with appropriate clearances are authorized to handle the data throughout the entire process.

- To date, there have been no known incidents of unauthorized access to or early release of the data.

- Copies of updated reports are stored at the central facility in a special locked cabinet and backup copies are stored at a GSA Records Center. The backup copies are maintained for three (3) cycles--current, plus two most recent months.

- A part of the final report, Section A, is created from some preliminary data. It must be available two days before the final data is transmitted so that analysis can be started. Updating the previous month's report requires preparation of the master tape. Certain other file tapes must be used in this process; these include Personnel Assignment data, Regional Projects data and Budget Status data.

- Each of the elements is considered critical to the final product. At the conclusion of each stage, checks are made for errors which might have been introduced. No major errors have ever been detected. Errors which have been found are restricted primarily to the new data tapes created by field offices.

- If the system were to be violated, or if the report were to be late, some adverse impact would be felt in the stock markets. There would be embarrassment to the Government at both national and international levels.

- The data is of such importance to "outside" individuals that relatively senior personnel could be tempted to obtain pre-release information or cause the final report to miss the established publication date.

- All personnel involved are continuously observed by their managers for any signs of attitude change, deterioration in performance, or other indications of situations that could result in breaches to the security of this project.

- All corrections, updates, or modifications to the software systems are closely monitored and tested before final approval and/or subsequent incorporation into the master system.

- Terminals in field offices are used by several branches of the agency for a number of different purposes.

The processing system consists of the six stages shown below:

Input	Process	Output
Stage 1-Data preparation Source data	key to tape verify duplicate microfilm destroy source doc	Source data tape + 1 copy microfilm
Stage 2-Data transmission Source data tape	transmit verify	Change data tape
Stage 3-File maintenance Mastertape (current) Change data tape	update verify duplicate tape	Master tape (new + 1 copy)
Stage 4-Section A creation Master tape Personnel assignment data Regional projects data Budget status data	calculate format	Section A report
Stage 5-Final report creation Master tape Personnel assignment data Regional projects data Budget status data	Same as Stage 4	Final report
Stage 6-Querying Master tape Personnel assignment data Regional projects data Budget status data	search read	video display

The worksheet for this system is shown in figure 4.

SYSTEM/APPLICATION Data Files	DATA INTEGRITY Modification (i)	(ALE)	(f)	Destruction (i)	(ALE)	(f)	DATA CONFIDENTIALITY (i)	(ALE)	(f)	PROCESSING AVAILABILITY 2 hrs (i) (f) (ALE)	24 hrs (i)(f) (ALE)	72 hrs (i)(f) (ALE)	COMMENTS
APPLICATION 100													
Source Documents	4		1	4		1	5	$3K	2[a]	---	---	---	a. key to tape, st. 1
Source data tape	4	$30K	4[a]	3		2	5	$30K	3[a]	---	---	---	a. key to tape, st. 1
Microfilm		----			----		5		3[a]	---	---	---	a. microfilm, st. 1
Change data tape	3	$300	3[a]	3	$300	3[a]	5	$300K	4[a]	---	6 3[a] $300K	---	a. transmit, st. 2
Master tape	5	$300	3	5	$300	3[a,b]	7	$300	4[a,b,c]	7 4[a,b,d] $30M	---	---	a. entire operation st. 4 b. entire operation st. 5 c. read, st. 6 d. power interrupt, op. shutdown
Personnel assignment data	5	$300	1	5	$300	1	5	$300	1	5 3[a] $30K	---	---	a. calculate, st. 4, 5
Regional projects data	3	$300	2[a]	3		1	4	$3K	2[a]	5 3[a] $30K	---	---	a. calculate, st. 4, 5
Budget status data	3		1	3		1	4		1	5 3[a] $30K	---	---	a. calculate, st. 4, 5

Figure 4. Risk Analysis Worksheet for Application 100

5.2.2 Application 870. This system is used to maintain and control the agency's plans and gross budgetary information for the most recent five years, the current year and the next five: ProgHist, CurrProg and AgPlans. The software consists of an agency developed program, PFiles, and a commercial proprietary program, WWWMod, which does the modeling required to choose the optimum course for future plans.

There are six video graphics terminals equipped with hard copy printers located in the offices of top management and a small control center with a large video screen in the office of the head of the agency to be used for displaying the results of on-line modeling at staff meetings. All files are mounted online during normal working hours. They are updated after every working day at 1:00 a.m. with the previous day's transaction--an average of ten except during February and August when processing time jumps from 1.8 hours a month to 4 hours a month.

The system consists of the three stages shown below:

Input	Process	Output
Stage 1-Daily file maintenance	(1:00 a.m., 1.8 hrs/mo except Feb & Aug - 4 hrs/mo)	
CurrProg	update files	CurrProg
PFiles	verify	
	duplicate	
Stage 2-Querying and modeling	(8:00 a.m. to 5:00 p.m. daily)	
AgPlans	search files	video display
CurrProg	read files	printout
WWWMod	calculate	
Stage 3-Semiannual report creation	(during working hours, February and August)	
AgPlans	calculate	MBO future report (2 copies only)
CurrProg	verify	AgPlans
ProgHist	format	ProgHist
WWWMod	update AgPlans	video display
PFiles	update ProgHist	
	verify	

The worksheet for this application is shown in figure 5.

5.3 Risk Analysis Team's Reasoning

The facts which emerged in the risk analysis process are described briefly to demonstrate the effectiveness of the technique and its capability for reducing gross apprehensions to manageable proportions.

5.3.1 Application 100. The team found that any losses which might occur at the field offices were minor and appeared under cursory examination to be of a nature which could be averted by implementing procedural measures. The largest losses which could occur in the system were related

SYSTEM/APPLICATION Data Files	DATA INTEGRITY						DATA CONFIDENTIALITY			PROCESSING AVAILABILITY			COMMENTS
	Modification			Destruction						2 hrs	24 hrs	72 hrs	
APPLICATION 870	(i)	(ALE)	(f)	(i)	(ALE)	(f)	(i)	(ALE)	(f)	(i)(f) (ALE)	(i)(f) (ALE)	(i)(f) (ALE)	
AgPlans	6	$300K	3	4	$300	2	7	$30M	4	---	---	---	
CurrProg	5	$30K	3	4	$300	2	6	$300K	3	---	---	---	
ProgHist	4	$300	2		-----			-----		---	---	---	
WWWMod	4	$3K	3	4	$300	2	4	$3K	3	---	---	---	
PFiles	4	$300	2	4	$300	2	4	$300	2	---	---	---	

Figure 5. Risk Analysis Worksheet for Application 870

directly to the data on the master tape and the availability of processing to convert the data on the master tape into the required report. It was obvious that safeguards for protecting these two areas would also have an umbrella effect on many of the other smaller concerns which were noted.

5.3.2 Application 870. The availability of the data files in this system, always on line during working hours, increased their vulnerability immeasurably. Upon inquiry, it became apparent to the team that there was no real need for such ready availability of the files. The files were used only infrequently by top management and processing availability was more of a convenience than a requirement. It became manifest that protection needs could be greatly reduced if the system were placed on a schedule or were made available only on 20 or 30 minutes notice, such details to be determined during the selection of safeguards.

6. CONCLUSION

It has been shown that a simple technique can be used to accomplish the desired result of risk analysis--determining where the vulnerabilities are in a system and how much should be spent to overcome them. The subsequent selection of safeguards can be done judiciously and expertly, using the facts gathered by the risk analysis team.

Appendix A

APPLICATION SYSTEM VULNERABILITIES

It will be useful to the team, as they consider data files by application, to be aware of the many undesirable events which can have serious consequences. A large number of situations to which systems are vulnerable are listed here, grouped according to common system organizational structures. The list is not intended to be all-inclusive but only to suggest the various kinds of vulnerabilities that may exist in each system.

- <u>ERRONEOUS OR FALSIFIED DATA INPUT</u>. Erroneous or falsified input data is the simplest and most common cause of undesirable performance by an applications system. Vulnerabilities occur wherever data is collected, manually processed, or prepared for entry to the computer.

  - Unreasonable or inconsistent source data values may not be detected.

  - Keying errors during transcription may not be detected.

  - Incomplete or poorly formatted data records may be accepted and treated as if they were complete records.

  - Records in one format may be interpreted according to a different format.

  - An employee may fraudulently add, delete, or modify data (e.g. payment vouchers, claims) to obtain benefits (e.g. checks, negotiable coupons) for himself.

  - Lack of document counts and other controls over source data or input transactions may allow some of the data or transactions to be lost without detection--or allow extra records to be added.

- Records about the data-entry personnel (e.g. a record of a personnel action) may be modified during data entry.

- Data which arrives at the last minute (or under some other special or emergency condition) may not be verified prior to processing.

- Records in which errors have been detected may be corrected without verification of the full record.

o <u>MISUSE BY AUTHORIZED END USERS</u>. End users are the people who are served by the ADP system. The system is designed for their use, but they can also misuse it for undesirable purposes. It is often very difficult to determine whether their use of the system is in accordance with the legitimate performance of their job.

  - An employee may convert Government information to an unauthorized use; for example, he may sell privileged data about an individual to a prospective employer, credit agency, insurance company, or competitor; or he may use Government statistics for stock market transactions before their public release.

  - A user whose job requires access to individual records in a file may manage to compile a complete listing of the file and then make unauthorized use of it (e.g. sell a listing of employees' home addresses as a mailing list.)

  - Unauthorized altering of information may be accomplished for an authorized end user (e.g. altering of personnel records).

  - An authorized user may use the system for personal benefit (e.g. theft of services).

  - A supervisor may manage to approve and enter a fraudulent transaction.

  - A disgruntled or terminated employee may destroy or modify records--possibly in such a way that backup records are also corrupted and useless.

  - An authorized user may accept a bribe to modify or obtain information.

o <u>UNCONTROLLED SYSTEM ACCESS</u>. Organizations expose themselves to unnecessary risk if they fail to establish controls over who can enter the ADP area, who can use the ADP system, and who can access the information contained in the system.

- Data or programs may be stolen from the computer room or other storage areas.

- ADP facilities may be destroyed or damaged by either intruders or employees.

- Individuals may not be adequately identified before they are allowed to enter ADP area.

- Remote terminals may not be adequately protected from use by unauthorized persons.

- An unauthorized user may gain access to the system via a dial-in line and an authorized user's password.

- Passwords may be inadvertently revealed to unauthorized individuals. A user may write his password in some convenient place, or the password may be obtained from card decks, discarded printouts, or by observing the user as he types it.

- A user may leave a logged-in terminal unattended, allowing an unauthorized person to use it.

- A terminated employee may retain access to ADP system because his name and password are not immediately deleted from authorization tables and control lists.

- An unauthorized individual may gain access to the system for his own purposes (e.g. theft of computer services or data or programs, modification of data, alteration of programs, sabotage, denial of services).

- Repeated attempts by the same user or terminal to gain unauthorized access to the system or to a file may go undetected.

o <u>INEFFECTIVE SECURITY PRACTICES FOR THE APPLICATION</u>. Inadequate manual checks and controls to insure correct processing by the ADP system or negligence by those responsible for carrying out these checks results in many vulnerabilities.

- Poorly defined criteria for authorized access may result in employees not knowing what information they, or others, are permitted to access.

- The person responsible for security may fail to restrict user access to only those processes and data which are needed to accomplish assigned tasks.

- Large funds disbursements, unusual price changes, and unanticipated inventory usage may not be reviewed for correctness.

- Repeated payments to the same party may go unnoticed because there is no review.

- Sensitive data may be carelessly handled by the application staff, by the mail service, or by other personnel within the organization.

- Post-processing reports analyzing system operations may not be reviewed to detect security violations.

- Inadvertant modification or destruction of files may occur when trainees are allowed to work on live data.

- Appropriate action may not be pursued when a security variance is reported to the system security officer or to the perpetrating individual's supervisor; in fact, procedures covering such occurrences may not exist.

o <u>PROCEDURAL ERRORS WITHIN THE ADP FACILITY</u>. Both errors and intentional acts committed by the ADP operations staff may result in improper operational procedures, lapsed controls, and losses in storage media and output.

Procedures and Controls:

- Files may be destroyed during data base reorganization or during release of disk space.

- Operators may ignore operational procedures for example, by allowing programmers to operate computer equipment.

- Job control language parameters may be erroneous.

- An installation manager may circumvent operational controls to obtain information.

- Careless or incorrect restarting after shutdown may cause the state of a transaction update to be unknown.

- An operator may enter erroneous information at CPU console (e.g. control switch in wrong position, terminal user allowed full system access, operator cancels wrong job from queue).

- Hardware maintenance may be performed while production data is on-line and the equipment undergoing maintenance is not isolated.

- An operator may perform unauthorized act for personal gain (e.g. make extra copies of competitive bidding reports, print copies of unemployment checks, delete a record from journal file).

- Operations staff may sabotage the computer (e.g. drop pieces of metal into a terminal).

- The wrong version of a program may be executed.

- A program may be executed using wrong data or may be executed twice using the same transactions.

- An operator bypasses required safety controls (e.g. write rings for tape reels).

- There may be inadequate supervision of operations personnel during off time shifts.

- Due to incorrectly learned procedures, an operator may alter or erase the master files.

- A console operator may override a label check without recording the action in the security log.

Storage Media Handling:

- Critical tape files are mounted without being write protected.

- Inadvertently or intentionally mislabeled storage media are erased. In a case where they contain back-up files the erasure may not be noticed until it is needed.

- Internal labels on storage media may not be checked for correctness.

- Files with missing or mislabeled expiration dates may be erased.

- Incorrect processing of data or erroneous updating of files may occur when card decks have been dropped, partial input decks are used, write rings mistakenly are placed in tapes, paper tape is incorrectly mounted, or wrong tape is mounted.

- Scratch tapes used for jobs processing sensitive data may not be adequately erased after use.

- Temporary files written during a job step for use in subsequent steps are erroneously released or modified through inadequate protection of the files or because of an abnormal termination.

- Storage media containing sensitive information may not get adequate protection because operations staff is not advised of the nature of the information content.

- Tape management procedures may not adequately account for the current status of all tapes.

- Magnetic storage media that have contained very sensitive information may not be degaussed before being released.

- Output may be sent to the wrong individual or terminal.

- Improperly operating output or post-processing units (e.g. bursters, decollators of multipart forms) may result in loss of output.

- Surplus output material (e.g. duplicates of output data, used carbon paper) may not be properly disposed of.

- Tapes and programs that label output for distribution may be erroneous or not protected from tampering.

o <u>PROGRAM ERRORS</u>. Applications programs should be developed in an environment that requires and supports complete, correct, and consistent program design, good programming practices, adequate testing, review, and documentation, and proper maintenance procedures. Although programs developed in such an environment will still contain undetected errors, programs not developed in this manner will probably be rife with errors. Additionally, programmers can deliberately modify programs to produce undesirable side-effects or they can misuse the programs they are in charge of.

  - Records may be deleted from sensitive files without a guarantee that the deleted records can be reconstructed.

  - Programmers may insert special provisions in programs that manipulate data concerning themselves (e.g. payroll programmer may alter his own payroll records).

  - Data may not be kept separate from code with the result that program modifications are more difficult and must be made more frequently.

  - Program changes may not be adequately tested before being used in a production run.

  - Changes to a program may result in new errors because of unanticipated interactions between program modules.

  - Program acceptance tests may fail to detect errors that only occur for unusual combinations of input (e.g. a program that is supposed to reject all except a specified set of values actually accepts an additional value).

  - Programs, the contents of which should be safeguarded, may not be identified and protected.

  - Code, test data with its associated output, and documentation for certified programs may not be filed and retained for reference.

  - Documentation for vital programs may not be safeguarded.

- Programmers may fail to keep a change log, to maintain back copies, or to formalize record keeping activities.

- An employee may steal programs he is maintaining and use them for personal gain (e.g. sale to a competitor, hold another organization for extortion).

- Poor program design may result in a critical data value being initialized twice. An error may occur when the program is modified to change the data value--but only changes it in one place.

- Production data may be disclosed or destroyed when it is used during testing.

- Errors may result when the programmer misunderstands requests for changes to the program.

- Errors may be introduced by a programmer who makes changes directly to machine code.

- Programs may contain hidden routines that disable or bypass security protection mechanisms. For example, a programmer inserts code into a program causing vital system files to be deleted as soon as he is terminated and his name no longer appears in the payroll file--i.e., he is terminated.

- Inadequate documentation or labeling may result in wrong version of program being modified.

o <u>OPERATING SYSTEM FLAWS</u>. Design and implementation errors, system generation and maintence problems, and deliberate penetrations resulting in modifications to the operating system can produce undesirable effects in the application system. Flaws in the operating system are often difficult to prevent and detect.

- User jobs may be permitted to read or write outside assigned storage area.

- Inconsistencies may be introduced into data due to simultaneous processing of the same file by two jobs.

- An operating system design or implementation error may allow a user to disable audit controls or to access all system information.

- The operating system may not protect a copy of information as thoroughly as it protects the original.

- Unauthorized modification to the operating system may allow a data entry clerk to enter programs and thus subvert the system.

- An operating system crash may expose valuable information such as password lists or authorization tables.

- Maintenance personnel may bypass security controls while performing maintenance work. At such times the system is vulnerable to errors or intentional acts committed by the maintenance personnel (e.g. microcoded sections of the operating system may be tampered with or sensitive information from on-line files may be disclosed).

- An operating system may fail to record that multiple copies of output have been made from spooled storage devices.

- An operating system may fail to maintain an unbroken audit trail.

- When restarting after a system crash, the operating system may fail to ascertain that all terminal locations which were previously occupied are still occupied by the same individuals.

- A user is able to get into monitor or supervisory mode.

- The operating system fails to erase all scratch space assigned to a job after the normal or abnormal termination of the job.

- Files are allowed to be read or written without having been opened.

o COMMUNICATIONS SYSTEM FAILURE. Information being routed from one location to another over communication lines is vulnerable to accidental failures and to intentional interception and modification by unauthorized parties.

Accidental Failures:

- Undetected communications errors may result in incorrect or modified data.

- Information may be accidentally misdirected to the wrong terminal.

- Communication nodes may leave unprotected fragments of messages in memory during unanticipated interruptions in processing.

- Communication protocol may fail to positively identify the transmitter or receiver of a message.

Intentional Acts:

- Communications lines may be monitored by unauthorized individuals.

- Data or programs may be stolen via telephone circuits from a remote job entry terminal.

- Programs in the network switching computers may be modified to compromise security.

- Data may be deliberately changed by individuals tapping the line (requires some sophistication, but is applicable to financial data).

- An unauthorized user may "take over" a computer communication port as an authorized user disconnects from it. Many systems cannot detect the change. This is particularly true in much of the currently available communication equipment and in many communication protocols.

- If encryption is used, keys may be stolen.

- A terminal user may be "spoofed" into providing sensitive data.

- False messages may be inserted into the system.

- True messages may be deleted from the system.

- Messages may be recorded and replayed into the system ("Deposit $100" messages).

Appendix B

REFERENCES AND SUGGESTED READING

1. Computer Security Guidelines for Implementing the Privacy Act of 1974, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication (FIPS PUB) 41, National Technical Information Service, Springfield, Virginia 22161 (1975).

2. Courtney, Robert H., Jr. and Orceyre, Michel J., Considerations in the Selection of Security Measures. To be published by the National Bureau of Standards.

3. Data Security Controls and Procedures--A Philosophy for DP Installations, G320-5649-00, IBM Corporation, White Plains, N.Y. (1976).

4. Disaster Preparedness, Office of Emergency Preparedness Report to Congress, Government Printing Office, Washington, D.C. 20402, Stock Number 4102-0006 (1972).

5. Glossary for Computer Systems Security, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication (FIPS PUB) 39, National Technical Information Service, Springfield, Virginia 22161 (1976).

6. Guide to Computer Security Inspection and Evaluation. To be published by the National Bureau of Standards.

7. Guidelines for ADP Physical Security and Risk Management, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication (FIPS PUB) 31, National Technical Information Service, Springfield, Virginia 22161 (1974).

8. Martin, James, Security, Accuracy and Privacy in Computer Systems, Prentice-Hall, Inc., Englewood Cliffs, N.J. (1973).

9. Parker, Donn B., Crime by Computer, Charles Scribner's Sons, New York (1976).

NBS-114A (REV. 7-73)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBSIR 77-1228	2. Gov't Accession No.	3. Recipient's Accession No.
4. TITLE AND SUBTITLE Automatic Data Processing Risk Assessment			5. Publication Date March 1977
			6. Performing Organization Code
7. AUTHOR(S) Susan K. Reed			8. Performing Organ. Report No. NBSIR 77-1228
9. PERFORMING ORGANIZATION NAME AND ADDRESS NATIONAL BUREAU OF STANDARDS DEPARTMENT OF COMMERCE WASHINGTON, D.C. 20234			10. Project/Task/Work Unit No.
			11. Contract/Grant No.
12. Sponsoring Organization Name and Complete Address *(Street, City, State, ZIP)* National Bureau of Standards Department of Commerce Washington, D.C. 20234			13. Type of Report & Period Covered Interim
			14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

This document presents a technique for conducting a risk analysis of an ADP facility and related assets. Risk analysis produces annual loss expectancy values based on costs and potential losses estimated by a management-appointed team from within the organization using and maintaining the ADP facility. The annual loss expectancy values are fundamental to the cost-effective selection of safeguards for the security of the facility. For the purpose of clarity, the ADP facility of a hypothetical Federal agency is used for an example. The characteristics and attributes which must be known in order to perform a risk analysis are described and the process of analyzing some of the assets is demonstrated, showing how the problem of risk analysis can be reduced to manageable proportions.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

ADP availability; annual loss expectancy; application system vulnerability; computer security; data confidentiality; data integrity; data security; physical security; procedural security; risk analysis; risk assessment; systems security

18. AVAILABILITY [X] Unlimited	19. SECURITY CLASS (THIS REPORT)	21. NO. OF PAGES
[ ] For Official Distribution. Do Not Release to NTIS	UNCLASSIFIED	36
[ ] Order From Sup. of Doc., U.S. Government Printing Office Washington, D.C. 20402, SD Cat. No. C13	20. SECURITY CLASS (THIS PAGE)	22. Price
[X] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151	UNCLASSIFIED	$4.00